

## UNITED STATES DISTRICT COURT

for the  
Southern District of OhioFILED  
RICHARD W. HAGEL  
CLERK OF COURT

2019 AUG 15 PM 4:01

U.S. DISTRICT COURT  
SOUTHERN DIST. OHIO  
DAYTON

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

Case No.

3:19mj506

AN ACCOUNT IDENTIFIED AS  
CNNRBETTS477@GMAIL.COM THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE LLC.

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section  
 18 U.S.C. § 922(g)(3)  
 18 U.S.C. § 922(a)(6)  
 18 U.S.C. § 924(a)(1)(A)  
 18 U.S.C. § 1001  
 21 U.S.C. § 844

## Offense Description

Possession of a firearm by an unlawful user of a controlled substance or by a person addicted to a controlled substance  
 false statement regarding firearms  
 false statement regarding firearms  
 false statement  
 unlawful possession of a controlled substance

The application is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



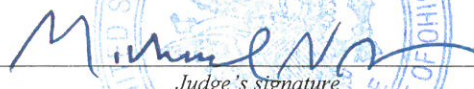
Applicant's signature

P. Andrew Gragan, Special Agent, FBI

Printed name and title

Sworn to before me and signed in my presence.

Date: 08/15/2019



Judge's signature

City and state: Dayton, Ohio

Hon. Michael J. Newman, U.S. Magistrate Judge

Printed name and title

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the account identified as **cnnrbetts477@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google LLC**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC (“Google”), regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A for the period of **January 1, 2013 to present**:

- a. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.
- b. All electronic files stored online via Google Drive, stored and presently contained in, or on behalf of the account described above.
- c. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.
- d. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above, including applications, subscribers’ full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers,

methods of payment, telephone numbers, addresses, change history, activity logs, device logs, and detailed billing and payment records.

- e. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.
- f. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.
- g. All existing printouts from original storage of all the electronic mail described above.
- h. All account contents previously preserved by Google, in electronic or printed form, including all e-mail, including attachments thereto, and Google Drive stored electronic files for the account described above).
- i. All subscriber records for any Google account associated by cookies, recovery email address, or telephone number to the account described above.
- j. All associated YouTube viewing history, uploading history, and other content.

2. All location information stored in the Google account.

3. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

4. The types of service utilized;



5. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

6. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken. Google is hereby ordered to disclose the above information to the government within **fourteen days** of service of this warrant.

## **II. Information to be Seized**

1. All records on the Account described in Attachment A that relate to violations of:

- 18 U.S.C. § 922(g)(3)
- 18 U.S.C. § 922(a)(6)
- 18 U.S.C. § 924(a)(1)(A)
- 18 U.S.C. § 1001
- 21 U.S.C. § 844

and involve **Connor Stephen BETTS (BETTS)** since **January 1, 2013**, including:

- a. Any information related to the purchase, use, or possession of firearms;
- b. Any information related to the purchase, use, or sale of controlled substances;
- c. Any information related to the types, amounts, and prices of controlled substances or firearms purchased, used, or trafficked as well as dates, places, and amounts of specific transactions;
- d. Any information related to sources of controlled substances or firearms (including names, addresses, phone numbers, or any other identifying information);

- e. Any information recording **BETTS'** schedule or travel from 2013 to the present;
- f. All bank records, checks, credit card bills, account information, and other financial records;
- g. Records of Internet Protocol addresses used;
- h. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF AN  
ACCOUNT IDENTIFIED AS  
CNNRBETTS477@GMAIL.COM THAT IS  
STORED AT PREMISES CONTROLLED  
BY GOOGLE LLC.

Case No. \_\_\_\_\_

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, P. Andrew Gragan, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Google LLC account that is stored at premises owned, maintained, controlled, or operated by Google LLC (“Google”), a multinational technology company that provides internet-related services and products, located at 1600 Amphitheatre Parkway, Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the user ID.

2. I am a Special Agent with the Federal Bureau of Investigation (“FBI”), Cincinnati Division. I have been employed as a Special Agent with the FBI since May 2016. I have received training in national-security investigations and criminal investigations, and I have conducted investigations related to international terrorism, white-collar crimes, drug trafficking, public corruption, firearms, and violent crimes. As part of these investigations, I have

participated in physical surveillance and records analysis, worked with informants, conducted interviews, served court orders and subpoenas, and executed search warrants.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 922(g)(3) (Possession of a firearm by an unlawful user of a controlled substance or by a person addicted to a controlled substance), 18 U.S.C. § 922(a)(6) (false statement regarding firearms), 18 U.S.C. § 924(a)(1)(A) (false statement regarding firearms); 18 U.S.C. § 1001 (false statement), and 21 U.S.C. § 844 (unlawful possession of a controlled substance), have been committed by **Conner BETTS** ("**BETTS**"). There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

#### **PROBABLE CAUSE**

5. On or about August 4, 2019, at approximately 1:00 a.m., Dayton Police Officers responded to an active shooter in the 400 block of East Fifth Street in Dayton, Ohio. Officers observed a male, later identified as **BETTS**, actively engaged in shooting into a crowd of individuals located at the 400 block of East Fifth Street in Dayton, Ohio, a city in the Southern District of Ohio.

6. The Officers were able to return fire towards the suspect in order to stop the threat. Multiple shots were fired, and **BETTS** was killed. At this time ten (10) people, including **BETTS**, are deceased resulting from the shooting, along with multiple individuals injured. The



injured were transported to multiple local area hospitals. **BETTS** was located on the scene wearing body-armor and headphones. Officers were able to identify the weapon as an assault rifle style firearm.

7. In the morning hours of August 4, 2019, the FBI was able to identify the shooter at the scene based on finger prints. The shooter was identified as **BETTS**.

8. On or about August 4, 2019 a Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Firearms Trace was conducted on the firearm used by **BETTS**, further described as an Anderson AM-15 5.56mm with serial number 18309695. The purchaser was **Connor Stephen BETTS**, with an address of 2250 Creekview Place, Bellbrook, Ohio, date of birth (DOB) of October 28, 1994, and a Social Security Number (SSN) with the last four digits of 6211. Ohio Bureau of Motor Vehicle (BMV) records reflect the same address, DOB, and last four digits of the SSN for **BETTS**.

9. Records obtained from a Dayton area Federal Firearm Licensed dealer included an ATF Form 4473, which based on my training and experience I know is required in order to complete the transaction of purchasing a firearm from a licensed dealer, for an Anderson Mfg model AM-15 receiver with serial number 18309695, which, based on information provided by ATF, was manufactured outside the state of Ohio. The transferee/buyer was listed on the ATF Form 4473 as **Connor Stephen BETTS** with the aforementioned address, DOB, and SSN. The transfer of the firearm from the dealer to **BETTS** was completed on April 12, 2019. **BETTS** listed **cnnrbetts477@gmail.com** (hereafter, "**ACCOUNT**") as his contact email address. Based on experience and training, I am aware that this email address is used by Google and its users as the means by which to identify user accounts with Google.

10. On or about August 5, 2019, a preservation letter was served to Google for the **ACCOUNT**.

11. Box 11e of ATF Form 4473 states, “Are you an unlawful user of, or addicted to, marijuana or any depressant, stimulant, narcotic drug, or any other controlled substance? Warning: The use or possession of marijuana remains unlawful under Federal law regardless of whether it has been legalized or decriminalized for medicinal or recreational purposes in the state where you reside.” The form contained warnings concerning the consequences of answering the questions on the form falsely. **BETTS’** Form 4473 was checked “No” in response to the question in box 11e.

12. Records from the same FFL dealer also showed an ATF Form 4473 for a Taurus Pt.111 G2C 9mm pistol with serial number TLR08219 was purchased by **BETTS** on November 23, 2018. The response to box 11e was checked “No.”

13. On or about August 4, 2019, Dayton Police Officers executed a search warrant, issued by the Dayton Municipal Court, on a 2007 Toyota Corolla bearing Ohio license plate number GNM1586. The vehicle was parked near the scene of the shooting and is believed to have been used by **BETTS** for transportation to the scene and for storage of the weapon he used in the shooting. Ohio BMV records show **BETTS’** father as the registered owner. Among other items, officers recovered a H&R 12 gauge Pardner Pump shotgun.

14. On or about August 4, 2019 an ATF Firearms Trace was conducted on the shotgun, further described as a Hawk Industries Inc. H&R Pardner Pump 12 gauge shotgun with serial number NZ897689. The purchaser was **Connor Stephen BETTS**, with an address of 2250 Creekview Place, Bellbrook, Ohio, date of birth (DOB) of October 28, 1994, and last four of

Social Security Number (SSN) 6211, identifying information consistent with the aforementioned BMV and other records.

15. Records obtained from a Dayton-area Federal Firearm Licensed (FFL) dealer included an ATF Form 4473 for a H&R Pardner 12 gauge shotgun with serial number NZ897689. The transferee/buyer listed on the ATF Form 4473 was **Connor Stephen BETTS** with the aforementioned address, DOB, and SSN. The transfer of the firearm from the dealer to **BETTS** was completed on June 21, 2019. **BETTS'** Form 4473 was checked "No" in response to the question in box 11e.

16. On or about August 4, 2019, **BETTS'** corpse was taken to the Montgomery County Coroner for autopsy. During the autopsy, Dayton Police Officers removed property from the pockets of **BETTS**, including an approximate three inch long black straw with a baggie attached to the end of it by a rubber band. Inside the baggie was a white powder, which the seizing officers, based on their training and experience, believe to be cocaine based on its appearance. The suspected cocaine was submitted to the Miami Valley Regional Crime Lab (MVRCL) for testing. MVRCL reported, on or about August 9, 2019, that the substance was cocaine.

17. On or about August 4, 2019, the FBI interviewed a friend of **BETTS**, who was with **BETTS** at the scene of the shooting and was shot and wounded by **BETTS**, and who for the purpose of this affidavit will be referred to as C.B. C.B. advised that around July 26 to 28, 2019, **BETTS** indicated to C.B. that he had relapsed with cocaine and it was not interacting well. C.B. also stated that **BETTS** had also invited him to go the range and shoot his AR, which C.B. did not do.



18. On or about August 4, 2019, a large national retail store, with a Federal Firearms License to deal in firearms, provided information to the FBI of weapon purchases made by **BETTS**. The weapons are further described as an H&R 1228 Pardner 12 gauge shotgun with serial number NZ682493, purchased on May 31, 2013; a DPMS Panther Arms, Inc, M4 Sportical .223-5.56 caliber rifle, with serial number L4017969, purchased on November 26, 2013; and a Mossberg 702 Plinkster 22LR rifle with serial number EML4019811, purchased on May 3, 2015. Records obtained from the retail store included ATF Form 4473s for all three firearms. Box 11e was checked “No” on all three Form 4473s.

19. On or about August 5, 2019, the FBI interviewed a high school girlfriend of **BETTS**, who for the purpose of this affidavit will be referred to as H.S. H.S. dated **BETTS** off and on in high school. She advised the FBI that **BETTS** had abused a number of drugs, including Adderall, Xanax, cocaine, and marijuana. H.S. indicated that **BETTS** purchased pills and cocaine from a manager at the restaurant **BETTS** worked at that time. H.S. advised that **BETTS** had told others he could sell cocaine to them, and that during 2013 to 2014, **BETTS** talked about having hallucinations and feeling like bugs were under his skin.

20. On or about August 5, 2019, the FBI interviewed another former, but more recent girlfriend of **BETTS**, who for the purpose of this affidavit will be referred to as C.J. C.J. knew **BETTS** since at least January 2019, having been classmates at a local college. C.J. dated **BETTS** from at least March 2019, until they severed their relationship in or about May 2019. C.J. indicated that **BETTS** was previously addicted to methamphetamine and was a recovering meth addict. **BETTS** had told her he quit “cold turkey” after going on vacation with his family and he was unable to obtain illegal narcotics.



21. On or about August 4 to 7, 2019, the FBI interviewed multiple individuals associated with **BETTS**. A co-worker, who for the purpose of this affidavit will be referred to as N.G., advised he was aware **BETTS** used to have a methamphetamine addiction approximately three years ago. A co-worker, who for the purpose of this affidavit will be referred to as K.G., advised that **BETTS** had told K.G. that he used to have a drug abuse problem during high school. When K.G. asked what type of drugs **BETTS** was abusing, **BETTS** mentioned huffing and cocaine. A bandmate of **BETTS**, who for the purpose of this affidavit will be referred to as J.C., advised that **BETTS** had told J.C. he used to use methamphetamine. A co-worker of **BETTS**, who for the purpose of this affidavit will be referred to as C.W., advised that **BETTS** had done methamphetamine in the past. C.W. believed **BETTS** had been clean for approximately four years. A co-worker of **BETTS**, who for the purpose of this affidavit will be referred to as A.G., believed that **BETTS** had a history of drug abuse.

22. On or about August 7, 2019, the FBI interviewed an acquaintance of **BETTS**, who for the purpose of this affidavit will be referred to as J.E. J.E. indicated that he and **BETTS** hung out at least once a month from 2014 through 2017. J.E. indicated that **BETTS** was hardly ever sober during this time and used heroin, cocaine, methamphetamine, and prescription narcotics. J.E. said that **BETTS** would often show up to his home “messed up.”

23. On or about August 7, 2019, the FBI interviewed a former co-worker of **BETTS**, who for the purpose of this affidavit will be referred to as E.S. E.S. advised that on or about August 2, 2019, at approximately 4:45p.m., **BETTS** came into her place of employment and bought a beer. Before he left, **BETTS** made the comment, “I just popped a xanny, we’ll see how it goes.” Based on my training and experience, I know that the term “xanny” is often used as street terminology for Xanax, a controlled substance.

24. On or about August 7, 2019, the FBI interviewed an acquaintance of **BETTS**, who for the purpose of this affidavit will be referred to as J.E. J.E. advised that during the timeframe he and **BETTS** were acquainted, which was late 2018, J.E. believed **BETTS** was using various drugs, including cocaine, methamphetamine, heroin, and molly.

25. On or about August 8, 2019, the FBI interviewed a friend of **BETTS**, who for the purpose of this affidavit will be referred to as E.K. E.K. informed the FBI that he and **BETTS** had done “hard drugs,” marijuana, and acid together four to five times a week during 2014 to 2015.

26. On or about August 8, 2019, E.K. was interviewed again by the FBI. E.K. acknowledged his purchase for **BETTS** of the following items used by **BETTS** in the August 4, 2019 shooting in Dayton: (1) body armor, (2) upper receiver of the AM-15 weapon, and (3) the 100-round double drum magazine. E.K. indicated that he purchased these items for **BETTS** – and stored them in E.K.’s apartment – to assist **BETTS** in hiding them from **BETTS**’ parents. E.K. indicated that approximately 10 weeks ago while in E.K.’s apartment, E.K. watched and helped **BETTS** assemble the AR-15 weapon used by **BETTS** in the August 4, 2019 shooting in Dayton. E.K. indicated that upon arrival of the drum magazine approximately 6 to 8 weeks ago, **BETTS** retrieved the assembled weapon, including the drum magazine, and took possession of it and the body armor at that time.

27. Based on my training and experience, I am familiar with the process by which individuals purchase, obtain, possess, and sell firearms and ammunition, and how they obtain, possess, sometimes grow, and use controlled substances. I know that individuals engaged in these activities often utilize email and other online and social media platforms and websites to communicate, including purchasing and planning the purchase of firearms and drugs, arranging

the subsequent sale and distribution of firearms and drugs, and discussing the use thereof. I also know that individuals engaged in illegal activity often maintain multiple email and social media accounts.

**BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY**

28. Based on my training and experience, I know that cellular devices, such as mobile telephones, are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called “cell sites,” which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

29. Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless Internet (“wi-fi”) access points if a user enables wi-fi connectivity. Wi-fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that functions as the name of the wi-fi network. In general, devices with wi-fi capability routinely scan their environment to determine what wi-fi access points are within range and will display the names of networks within range under the device’s wi-fi settings.

30. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves



to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device's transmission range, to which it might connect.

31. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system ("GPS") technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app's operation.

32. Based on my training and experience, I know Google is a company that, among other things, offers an operating system ("OS") for mobile devices, including cellular phones, known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

33. In addition, based on my training and experience, I know that Google offers numerous online-based services, including email (Gmail), navigation (Google Maps), search engine (Google), online file storage (including Google Drive, Google Photos, and Youtube), messaging (Google Hangouts and Google Allo), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging, require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google, and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and Youtube, can be used while signed in to a Google account, although some aspects of these services can be used even without being signed in to a Google account.



34. In addition, based on my training and experience, I know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be synced across the various devices on which they may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices.

35. Based on my training and experience, I know that, in the context of mobile devices, Google's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

36. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. In addition, I know that Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google account associated with the Android device and/or that is signed in via the relevant Google app. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about wi-fi access points and Bluetooth beacons within range of the mobile device.

37. Based on my training and experience, I also know that Google collects and retains information about the user's location if the user has enabled Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol address at the time they engage in certain Internet- and app- based activity and associates this information with the Google account associated with the Android device and/or that is signed in with the relevant Google app.

38. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products as described above, mobile devices that were in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can inculpate or exculpate a Google account holder by showing that s/he was, or was not, near a given location at a time relevant to the criminal investigation.

39. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

40. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

41. As explained herein, information stored in connection with a Google account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Google user's IP log, stored electronic communications, and other data retained by Google, can indicate who has used or controlled the Google account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Google account at a relevant time. Further, Google account activity can show how and when the account was accessed or used. For example, as described herein, Google logs the Internet Protocol (IP) addresses from which users access their



accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Google access, use, and events relating to the crime under investigation. Additionally, Google builds geo-location into some of its services. This geographic and timeline information may tend to either inculcate or exculpate the Google account owner. Last, Google account activity may provide relevant insight into the Google account owner's state of mind as it relates to the offenses under investigation. For example, information on the Google account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

42. Therefore, the computers of Google are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Google, such as account access information, transaction information, and other account information.

**INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

43. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.




**CONCLUSION**

44. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, which will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

45. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).


46. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

Respectfully submitted,



P. Andrew Gagan  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me  
on August 15, 2019, in Dayton, Ohio.



HON. MICHAEL J. NEWMAN  
UNITED STATES MAGISTRATE JUDGE



**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with the account identified as **cnnrbetts477@gmail.com** that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Google LLC**

To the extent that the information described in Attachment A is within the possession, custody, or control of Google LLC (“Google”), regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for each account or identifier listed in Attachment A for the period of **January 1, 2013 to present**:

- a. All available account contents from inception of account to present, including e-mails, attachments thereto, drafts, contact lists, address books, and search history, stored and presently contained in, or maintained pursuant to law enforcement request to preserve.
- b. All electronic files stored online via Google Drive, stored and presently contained in, or on behalf of the account described above.
- c. All transactional information of all activity of the electronic mail addresses and/or individual account described above, including log files, dates, times, methods of connecting, ports, dial-ups, and/or locations.
- d. All business records and subscriber information, in any form kept, pertaining to the electronic mail addresses and/or individual accounts described above, including applications, subscribers’ full names, all screen names associated with the subscribers and/or accounts, all account names associated with the subscribers,

methods of payment, telephone numbers, addresses, change history, activity logs, device logs, and detailed billing and payment records.

- e. All records indicating the services available to subscribers of the electronic mail addresses and/or individual account described above.
- f. All search history records stored and presently contained in, or on behalf of the account described above including, if applicable, web and application activity history (including search terms), device information history, and location history.
- g. All existing printouts from original storage of all the electronic mail described above.
- h. All account contents previously preserved by Google, in electronic or printed form, including all e-mail, including attachments thereto, and Google Drive stored electronic files for the account described above).
- i. All subscriber records for any Google account associated by cookies, recovery email address, or telephone number to the account described above.
- j. All associated YouTube viewing history, uploading history, and other content.

2. All location information stored in the Google account.

3. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

4. The types of service utilized;



5. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files; and

6. All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken. Google is hereby ordered to disclose the above information to the government within **fourteen days** of service of this warrant.

## **II. Information to be Seized**

1. All records on the Account described in Attachment A that relate to violations of:

- 18 U.S.C. § 922(g)(3)
- 18 U.S.C. § 922(a)(6)
- 18 U.S.C. § 924(a)(1)(A)
- 18 U.S.C. § 1001
- 21 U.S.C. § 844

and involve **Connor Stephen BETTS (BETTS)** since **January 1, 2013**, including:

- a. Any information related to the purchase, use, or possession of firearms;
- b. Any information related to the purchase, use, or sale of controlled substances;
- c. Any information related to the types, amounts, and prices of controlled substances or firearms purchased, used, or trafficked as well as dates, places, and amounts of specific transactions;
- d. Any information related to sources of controlled substances or firearms (including names, addresses, phone numbers, or any other identifying information);

- e. Any information recording **BETTS'** schedule or travel from 2013 to the present;
- f. All bank records, checks, credit card bills, account information, and other financial records;
- g. Records of Internet Protocol addresses used;
- h. Records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.